Lesson 6. Protecting Your Privacy

Lesson Purpose

> To provide strategies for protecting your privacy when using passwords, ATMs and credit cards, or shopping online.

Learning Objectives

> Participants will be able to:
> - Recognize transactions and practices that result in vulnerability to fraud and/or identity theft.
> - Identify specific strategies to reduce vulnerability to fraud and/or identity theft.

Materials

> Presentation: Protecting Your Privacy
>
> Handout(s):   *"Protecting Your Privacy: Keeping an Eye on Your Private Information"*
>
> Supplement: Online Privacy Guide – download at www.epic.org/privacy/tools.html

Related Resources

> National Crime Prevention Council, www.ncpc.org
> The Electronic Privacy Information Center, www.epic.org/privacy

Lesson Plan

Time	Main Points	Slide
	Introduction	
5 min.	**Background** E-mail, the Internet, ATMs, computer banking and credit cards make our lives more efficient. However, the more we use technology the more difficult it becomes to keep private information confidential. Electronic transactions can leave you vulnerable to fraud and other crimes.	1 – 2
	Briefly describe a recent, local example of identity theft.	
	Crime can be random, but there are steps you can take to limit your chances of becoming a victim. Being aware of the threat of crime -- and staying alert to what you can do to prevent it -- will go a long way toward making your electronic transactions safe and private. Today we will look at practices that increase our vulnerability to fraud and/or identity theft and review specific strategies to reduce that vulnerability.	2
	Distribute the Handout "Protecting Your Privacy."	

Time	Main Points	Slide
	Presentation	
4 min.	**Passwords** ▪ Credit cards, bank/ATM and Internet accounts often require the use of a password. ▪ The worst passwords - ones that come to mind first, such as your name or the names of friends, relatives, pets, or your street address, etc.) ▪ Best passwords: mix numbers with upper and lowercase letters. If they can't be found in the dictionary, it is even better. ▪ Don't be a "Joe" -- someone who uses his own name as a password. ▪ The weakest link in a security system is the human element. ▪ The fewer people who have access to your codes and passwords, the better.	3
	Avoid breaks in your security by: ▪ Changing your password regularly. ▪ Memorizing your password. ▪ Setting up a special account or setting aside a different computer at work for temporary help and other unauthorized users. ▪ If you are given the option of letting your computer or a Web site remember a password for you, don't use it. ***Don't send confidential, financial or personal information on your e-mail system***.	4
2 min.	**Shopping in Cyberspace** Ordering merchandise from the Internet is a trend of the future. You can prevent problems before they occur by: ▪ Doing business with companies you know and trust. ▪ Understanding the offer. Look carefully at the products or services the company is offering. ▪ Using a secure browser that will encrypt or scramble purchase information. ▪ Never giving a bank account number, credit card number or other personal information to anyone you do not know or have not followed-up on.	5

Time	Main Points	Slide
5 min.	**Using ATMs, Long Distance Phone Services and Credit Cards** <u>Protect your Personal Identification Number (PIN)</u> ▪ Your PIN should be memorized, secured and not given to anyone, not even family members or bank employees. The fewer people who have access to your PIN, the better. ▪ Never write your PIN on ATM or long distance calling cards. Don't write your PIN on a piece of paper and place it in your wallet. If your wallet or card is ever lost or stolen, someone who finds it will have everything he or she needs to remove funds from your account, make unauthorized debit purchases or run up your long distance phone bill.	6
	<u>Protect Your ATM Cards</u> ▪ An ATM card should be regarded as though it were cash. Avoid providing card and account information to anyone over the telephone. ▪ When making a cash withdrawal at an ATM, immediately remove the cash as soon as the machine releases it. Put the cash in your pocket and wait until you are in a secure location before counting it. Never use an ATM in an isolated area or where people are loitering. ▪ Be sure to take your receipt to record transactions and match them against monthly statements. Dishonest people can use your receipt to get your account number. Never leave the receipt at the site.	7
8 min.	<u>Protect Your Credit Cards</u> ▪ Only give your credit card account number to make a purchase or reservation you have initiated. Never give this information over a cellular phone. ▪ Never give your credit card to someone else to use on your behalf. ▪ Watch your credit card after giving it to store clerks to protect against extra imprints being made. ▪ Destroy any carbons. Do not discard into the trash can at the purchase counter. Keep charge slips in a safe place. ▪ Protect your purse or wallet, especially when traveling, or when you find yourself in crowded situations.	8
	▪ Save all receipts, and compare them to your monthly statement. Report any discrepancies immediately! ▪ Keep a master list in a secure place at home, with all account numbers and phone numbers for reporting stolen or lost cards. <u>Lost or Stolen Cards</u> ▪ Always report lost or stolen cards to the issuing company immediately. This limits any unauthorized use of your card and permits the company to begin the process of issuing a new card.	9

Time	Main Points	Slide
2 min.	**Summarizing** • Create and use passwords and PINs wisely. • Use care when shopping online. • Protect your credit cards. If lost, report missing cards immediately.	10
Practice/feedback		
10 min.	Have participants review the list of tips for protecting their privacy, in their handout. Ask them to place a checkmark (√) beside the things they now do and to place an asterisk (*) beside the things that they need to begin doing. Give participants 5 to 7 minutes to complete this review. The instructor should circulate among participants during this time. Conclude the activity by asking a couple of volunteer participants to share what they learned from the review. The instructor should reinforce prevention strategies and key learning points.	11
Evaluation		
10 min.	**Set-up** We have a few minutes for questions and additional discussion. While we're doing that, we have a brief evaluation form we'd like for you to complete and leave with us. Your name is not required, but your feedback is very important. It will help us improve our presentation and program. Distribute evaluation forms and ask for questions or additional comments on what has been presented. Promote group discussion by encouraging audience members to help respond to questions. Use questions as an opportunity to clarify and reinforce key learning objectives. **Wrap-up** • Thank the audience for their attention and participation. • Express appreciation to the sponsoring organization for the opportunity to speak. • Remind them to leave evaluation forms.	12

6. Protecting Your Privacy

Please tell us what you think about this lesson by circling the numbers that most closely reflect your opinions.

After this lesson . . .	Strongly Disagree	Disagree	Agree	Strongly Agree
a) I am better able to recognize transactions and practices that result in vulnerability to fraud and/or identity theft.	1	2	3	4
b) I know more strategies to protect credit card information.	1	2	3	4
c) I know more strategies to reduce the likelihood of fraud and/or identity theft when using passwords and PINs.	1	2	3	4
d) I am now more likely to report activities or inquiries involving my private information that are suspicious.	1	2	3	4
About this lesson . . .				
e) The information presented was valuable.	1	2	3	4
f) The lesson was presented in a clear and understandable manner.	1	2	3	4
g) Lesson activities and discussion were helpful.	1	2	3	4
h) I would recommend this lesson to others.	1	2	3	4

What was the most valuable thing you learned?

Please give one example of how you plan to use the information presented in this lesson.

How could this lesson be improved?